In the Claims:

1. (previously presented) A N-dimensional biometric security system comprising

a station for receiving information representative of a user from the user and generating a signal responsive thereto;

a first data base having a plurality of words and language rules for generating one-time challenge phrases;

a second data base having biometric models of the user therein; and

a controller to receive and validate said signal as representative of the user, said controller communicating with said first data base for randomly generating a one-time challenge phrase from said plurality of words and language rules in said first data base and delivering said one-time challenge phrase to said station for the user to speak in response to validation of said signal, and said controller communicating with said station

to receive a spoken response from the user to said delivered one-time challenge phrase and to generate a second signal representative of the spoken response,

to process said second signal for speaker recognition and to issue a first validation signal in response to a match between said second signal and said stored biometric model,

to process said second signal for speech recognition and to issue a second validation signal in response to a match between said second signal and said one-time challenge phrase, and

to validate the spoken response to said one-time challenge phrase as representative of the user in response to receiving said first validation signal and said second validation signal.

2.(previously presented) A method of identifying and validating a user comprising the steps of

initially inputting information representative of the user at a station;

generating a signal responsive to the information;

receiving and validating the signal as representative of the user;

thereafter generating and delivering a randomly generated one-time challenge phrase at said station for the user to speak in response to validation of said signal;

generating a second signal representative of a spoken response to said challenge phrase;

thereafter receiving and simultaneously processing the second signal for speaker verification and for speech recognition and issuing a first validation signal in response to speaker verification and a second validation signal in response to speech recognition; and

validating the second signal as representative of the user in response to issuance of said first validation signal and said second validation signal.

3. (canceled)

4. (previously presented) A N-dimensional biometric security system comprising

a station for receiving input information representative of a user from the user and generating a first signal responsive thereto;

a first data base for storing a plurality of words and language rules for generating one-time challenge phrases corresponding to the user;

a second data base for storing a biometric model of each of a multiplicity of users; and

a controller for receiving and validating said first signal as representative of one of said multiplicity of users, said controller being operatively connected to said first data base to generate and deliver a one-time randomly generated challenge phrase to said station in response to said first signal for the user to speak,

said controller communicating with said station to receive and compare a spoken response to said challenge phrase with said challenge phrase to verify said spoken response as matching said challenge phrase and to compare said spoken response to said stored biometric model of said one user and for validating said spoken response as representative of said one user in response to a match between said spoken response and said stored biometric model of said one user, said controller issuing an authentication signal in response to a verification of said spoken response as matching said challenge phrase and a validation of said spoken response as representative of said one user.

5. (currently amended) A method of identifying and validating a user comprising the steps of

receiving information representative of a user from the user at an input station and generating a first signal responsive thereto;

storing a plurality of words and language rules for generating one-time challenge phrases in a first data base;

storing a biometric model of each of a multiplicity of users in a second data base;

generating a one-time ~~word~~ challenge phrase from said stored plurality of words and forwarding said ~~word~~ challenge phrase to said station in response to said first signal as a challenge phrase for the user to speak;

receiving a spoken response to said challenge phrase;

comparing said spoken response to said challenge phrase to verify said spoken response as matching said challenge phrase;

comparing said spoken response to the stored biometric models for validating said spoken response as representative of said one of said users in response to a match between said spoken response and said stored biometric model of said one of said users; and

issuing an authentication signal in response to a verification of said spoken response as matching said challenge phrase and a validation of said spoken response as representative of said one of said users.

6. (previously presented) A method as set forth in claim 5 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

7. (previously presented) A method as set forth in claim 2 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

8. (new) A method as set forth in claim 2 further comprising the step of establishing a session time out limit in response to validating of said first signal as representative of the user.

9. (new) A method as set forth in claim 2 wherein said randomly generated one-time challenge phrase makes sense and is simple to say.

10. (new) A method as set forth in claim 2 wherein said randomly generated one-time challenge phrase is a language subset specific to a subject area.

11. (new) A method as set forth in claim 5 further comprising the step of establishing a session time out limit in response to validating of said first signal as representative of

the user.

12. (new) A method as set forth in claim 5 wherein said randomly generated one-time challenge phrase makes sense and is simple to say.

13. (new) A method as set forth in claim 5 wherein said randomly generated one-time challenge phrase is a language subset specific to a subject area.

14. (new) A method as set forth in claim 5 further comprising the steps of encrypting and digitally signing a spoken response to said challenge phrase prior to said step of comparing said spoken response to the strored biometric models.